УДК 002.001+007.57

О.О. Варламов
Корпорация «Электронный архив», г. Москва, Россия
OVarlamov@elar.ru; www.elar.ru; ovar@narod.ru; www.ovar.narod.ru

Компьютерная разведка и создание АС до класса защищенности 1Г на основе сертифицированного ПС «ЭЛАР Саперион»

В статье исследованы возможности и перспективы создания защищенных от технической компьютерной разведки автоматизированных систем на примере системы управления информационными ресурсами «ЭЛАР Саперион».

Введение

В настоящее время актуальным является перевод всех бумажных документов и архивов в электронный вид, а также создание автоматизированных систем (АС) управления информационными ресурсами. Подчеркнем, что в последнее время это направление информационных технологий (ИТ) развивается очень быстро. Без сомнений, внедрение ИТ имеет целый ряд преимуществ и принципиально важных новых возможностей. Однако, учитывая развитие средств технической разведки, необходимо особое внимание уделять вопросам защиты информации, особенно ограниченного доступа. Практически все организации и предприятия заинтересованы в надежной защите информации, хранящейся и обрабатываемой в электронном виде.

Постановка задачи

Решаемая задача – анализ конкретных научно-практических аспектов создания защищенных АС и электронных архивов (ЭА), например, на основе программного обеспечения «ЭЛАР Саперион». Проанализируем его назначение и функции, а также возможные угрозы от всех 9 типов компьютерной разведки. Затем определим пути и основные этапы создания электронных архивов и АС до класса защищенности 1Г на основе системы управления информационными ресурсами «ЭЛАР Саперион», сертифицированной по НДВ-4. Опишем текущее состояние, перспективы развития и возможности достижения поставленной цели: создания АС по требованиям 1Г для обработки конфиденциальной информации.

Назначение и основные функции «ЭЛАР Саперион»

Прежде всего, проанализируем назначение и основные функции системы управления электронными информационными ресурсами «ЭЛАР Саперион». Программное средство «ЭЛАР Саперион» – это полнофункциональная платформа для создания АС управления электронными информационными ресурсами, формирующими в совокупности электронный архив документов, обработки запросов пользователей на поиск и просмотр документов, распознавания электронных образов текстовых документов, хра-

нящихся в электронном архиве, обеспечения полнотекстового поиска электронных образов документов, обеспечения комплектования, формирования, оформления и хранения архивных дел и документов и их поиска в информационной базе электронного архива.

«ЭЛАР Саперион» – мощная и широко используемая система для решения различных задач по работе с документами. САПЕРИОН предоставляет все возможности по созданию электронных информационных ресурсов (ИР), управлению ими, эффективному их использованию и развитию в масштабе организации.

«ЭЛАР Саперион» обеспечивает надежную управляемость крупным информационным ресурсом:

1. Автоматизацию процесса наполнения электронных архивов реальными документами (поддержка потокового ввода, загрузка одиночных документов).
2. Регистрацию документов (ручное и автоматическое индексирование).
3. Надежное и защищенное хранение документов, сохранение всех версий электронного документа.
4. Оперативный доступ к документам: быстрый поиск необходимых документов, многообразие форм поиска.
5. Интеграцию с другими информационными системами для импорта документа и его регистрационной информации, а также обеспечения доступа к документам через интерфейс этих систем.
6. Управление доступом пользователей к документам и регистрацию всех операций, которые производились с документами.
7. Предоставление статистической информации о документах, автоматизацию отчетности.
8. Гарантированная защита как от случайного, так и от умышленного уничтожения электронного информационного ресурса.
9. Высочайший уровень безопасности информации благодаря развитой системе доступа и кодирования данных.
10. Регламентация прав доступа не только к документам, но также к отдельным страницам документа или его фрагментам.
11. Возможность просмотра архивных копий документов, которые были удалены, а также и многое другое.

Передовая, высокотехнологичная система управления документами «ЭЛАР Саперион», построенная по принципу «все в одном», гарантирует безопасную и непрерывную обработку документов на всех стадиях – от сканирования до архивного хранения.

С точки зрения обеспечения безопасности информации необходимо подчеркнуть, что для хранения базы документов используется собственный формат (метафайл), который не может быть прочитан или изменён извне. Индексная информация хранится в одной из промышленных СУБД (MS SQL, Oracle, DB/2, Informix, Sybase и т.д.), при этом «ЭЛАР Саперион» берет на себя задачу администрирования соответствующей СУБД.

Система «ЭЛАР Саперион» имеет средства прямой поддержки специализированных архивных накопителей, позволяющих существенно расширить объем доступной памяти. Благодаря этому размер электронного информационного ресурса неограничен – можно использовать в качестве хранилища архива несколько RAID-массивов, специализированных архивных накопителей (DVD/BD/UDO).

Для исключения рисков, связанных с потерей, повреждением или уничтожением данных и документов и обеспечения катастрофоустойчивости, предоставляется возможность управлять миграцией данных в соответствии с заданными политиками и зеркалирования архивной базы данных. После любых сбоев и катастроф данные могут быть полностью восстановлены в течение нескольких минут.

Компьютерная разведка и ее источники информации

Общепризнано, что **под компьютерной разведкой** (КпР) не достаточно понимать только получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования [1]. В настоящее время КпР – это добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [2]. Существует три типа источников информации для КпР: 1) данные, сведения и информация обрабатываемые, в т.ч. передаваемые и хранимые, в компьютерных системах и сетях; 2) характеристики программных, аппаратных и программно-аппаратных комплексов; 3) характеристики пользователей компьютерных систем и сетей.

Исходя из основных функций, получаем, что ЭА на основе «ЭЛАР Саперион» соответствуют первому типу источников информации. Принципиально важно, что компьютерные системы являются многоуровневыми. Например, в эталонной модели взаимодействия открытых систем (ЭМВОС) выделяют семь уровней. На одинаковых компьютерах можно устанавливать совершенно различные программные комплексы для выполнения разнообразных задач. И, наоборот, на аппаратно разных физических компьютерах можно устанавливать одинаковые программные среды и комплексы для решения однотипных задач.

Многоуровневое построение обуславливает наличие на одной физической среде нескольких различных: объектов защиты, сред передачи данных и средств добывания информации, т.е. различных «виртуальных технических каналов утечки информации». «ЭЛАР Саперион» является программным обеспечением, работает на прикладном уровне (уровень приложений), т.е. над операционными системами, которые реализуют определенные функции защиты информации.

Таким образом, к ЭА не могут предъявляться требования по защите информации, относящиеся к другим уровням компьютерных технических каналов утечки информации.

Девять видов компьютерной разведки

По принципам построения программно-аппаратных комплексов, каналам утечки информации и функциональному предназначению выделяют [2], [3]: **техническую компьютерную разведку**, обеспечивающую добывание информации из компьютерных систем и сетей; характеристик их программно-аппаратных средств и пользователей, которая включает в себя 9 видов:

1) **семантическую**, обеспечивающую добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;

2) **алгоритмическую**, использующую программно-аппаратные закладки и недекларированные возможности для добывания данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;

3) **вирусную,** обеспечивающую добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;

4) **разграничительную**, обеспечивающую добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе несанкционированного доступа (НСД) к информации, а также реализация несанкционированного доступа при физическом доступе к похищенным компьютерам или машинным носителям информации (МНИ);

5) **сетевую**, обеспечивающую добывание данных из компьютерных сетей, путем реализации зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий;

6) **потоковую**, обеспечивающую добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров;

7) **аппаратную**, обеспечивающую добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами ТКУ;

8) **форматную**, обеспечивающую добывание информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов представления, передачи и хранения добытых данных в сведения, а затем в информацию для последующего ее представления Заказчику;

9) **пользовательскую**, обеспечивающую добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка).

Анализ возможности защиты информации электронных архивов от 9 видов компьютерной разведки

Проанализируем возможности защиты информации электронных архивов от указанных видов компьютерной разведки. Отметим, что в некотором смысле электронные архивы наиболее близки с точки зрения информационной безопасности (ИБ) к классу систем управления базами данных (СУБД).

Семантическая разведка занимается анализом фактографической информации и представляет собой угрозу для «ЭЛАР Саперион». Следовательно, необходимо предусмотреть защиту от этой разведки.

Алгоритмическая разведка на уровне программных закладок и недекларируемых возможностей представляет собой угрозу для любого программного обеспечения, включая и «ЭЛАР Саперион». Основным средством защиты от этого является сертификация и проверка на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля, т.к. анализируем только защиту конфиденциальной информации.

Вирусная разведка представляет собой угрозу для программного обеспечения, но для противодействия ей существуют специализированные средства, работающие независимо от программного обеспечения прикладного уровня. Следовательно, непосредственно к «ЭЛАР Саперион» такие требования не предъявляются.

Разграничительная разведка является важной угрозой как для баз данных, так и для электронных архивов. Причем защита от нее должна быть встроена непосредственно в сам программный продукт, либо необходимо встраивать внешние средства противодействия разграничительной разведке и не допущения несанкционированного доступа к конфиденциальной информации. В случае «ЭЛАР Саперион» такие средства есть, но для подтверждения эффективности их работы необходимо пройти сертификацию по требованиям РД Гостехкомиссии на «СВТ не менее 5 уровня». Отметим, что «ЭЛАР Саперион» позволяет разграничивать доступ даже к отдельным частям документов и внедрять внешние средства криптографии и электронно-цифровой подписи (ЭЦП), которые также повышают уровень противодействия разграничительной разведки.

Сетевая разведка также представляет собой большую угрозу для электронных архивов, но средства защиты от нее должны располагаться на сетевом уровне взаимодействия, где разработаны специальные аппаратные, программные и программно-аппаратные средства. В целом, непосредственно, к «ЭЛАР Саперион» эти требования не применимы, а относятся к защите всей АС.

Потоковая разведка работает на том же уровне, что и сетевая. Следовательно, к «ЭЛАР Саперион» эти требования не применимы, а относятся к защите всей АС. Для этого должны применяться специальные программно-аппаратные комплексы. Впрочем, отдельного исследования требует оценка необходимости защиты от потоковой разведки конфиденциальной информации. С учетом критерия стоимости самой подсистемы защиты информации, достаточно низких рисков и отсутствия явно сформулированных требований руководящих документов (РД Гостехкомиссии – ФСТЭК России), целесообразно оставить на усмотрение Заказчиков решение этого вопроса в зависимости от их субъективной оценки важности и критичности угроз потоковой разведки для них.

Аппаратная разведка направлена для получения информации об аппаратуре, т.е. уровень «железа», к которому «ЭЛАР Саперион» явно не относится. Следовательно, аппаратная разведка непосредственно для «ЭЛАР Саперион» не представляет угрозы и не требует отдельных мер защиты.

Форматная разведка представляет угрозу для «ЭЛАР Саперион». Однако специальных явно сформулированных требований руководящих документов (РД Гостехкомиссии – ФСТЭК России и ФСБ России), за исключением криптографических средств, не существует. Отметим, что в «ЭЛАР Саперион» разработчиком приняты специальные меры, затрудняющие реализацию угроз форматной разведки. Например, применяется «фирменное» преобразование (кодирование) информации в специальный внутренний формат для создания специальных записей, называемых «медии». Кроме того, «ЭЛАР Саперион» позволяет внедрять внешние криптографические средства противодействия форматной разведке. При необходимости, Заказчик может применять различные средства защиты информации, вплоть до сертифицированных российских криптографических средств защиты информации, типа «Крипто-Про».

Пользовательская разведка непосредственно не угрожает на уровне функционирования «ЭЛАР Саперион». Если Заказчику необходимо, то надо защищаться от этой разведки на других уровнях и специальными средствами. Отметим, что для «аттестации АС 1Г» в настоящее время требования по защите от пользовательской разведки не предъявляются. Следовательно, Заказчик сам вправе определить как защищать свою конфиденциальную информацию от пользовательской разведки.

Возможные действия поставщика программного обеспечения для аттестации АС Заказчика

Для аттестации по АС 1Г выдвигается довольно много требований, которые напрямую не относятся к программному обеспечению, но должны быть выполнены Заказчиком независимо от специфики АС. С точки зрения поставщика программного обеспечения «ЭЛАР Саперион» невозможно реализовать защиту от многих угроз. Это обусловлено тем, что такие угрозы не распространяются непосредственно на «ЭЛАР Саперион», хотя могут воздействовать опосредованно, например, вирусы через операционную систему.

Проанализируем, какие действия может выполнить поставщик «ЭЛАР Саперион» (или любого другого подобного программного обеспечения) для того, чтобы Заказчик мог аттестовать свою АС по требованиям 1Г.

Кратко напомним наиболее важные для решения этой задачи исходные положения. Для обработки информации ограниченного доступа необходимо обеспечить это самое «ограничение доступа», т.е. информационную безопасность (ИБ). Отметим, что если нет ограничения доступа к информации, то и нет требований по ее защите.

Есть два основных процесса: сертификация и аттестация.

Сертификация – это проверка отдельных компонентов и составных частей автоматизированных систем (АС). Аттестация – это испытание, в целом, АС, собранных из сертифицированных компонентов. Если нет сертификатов, то нельзя проводить аттестацию. Обрабатывать информацию ограниченного доступа разрешается только на соответствующим образом аттестованных АС с соблюдением всех ограничений и рекомендаций.

Итак, до любой аттестации АС необходимо провести сертификацию или использовать ранее сертифицированные компоненты ПО. В реальной жизни всё немного сложнее и есть разные варианты. Таким образом, поставщик программного обеспечения может только (План ИБ):

1) провести необходимую обязательную сертификацию по НДВ;

2) для сложного программного обеспечения, в котором есть встроенные средства защиты информации (операционные системы, СУБД и т.п.), провести сертификацию по СВТ;

3) показать работоспособность на необходимом Заказчику аппаратном обеспечении («железо»), которое при необходимости проходит специальные проверки и исследования;

4) обеспечить взаимодействие своего программного обеспечения с необходимым Заказчику сертифицированным программным обеспечением (операционные системы, СУБД и т.п.);

5) обеспечить совместимость с другими внешними средствами защиты информации (криптография и ЭЦП).

Сертификация НДВ. Обеспечение ИБ основывается на создании «безопасной зоны», которая охраняется по ее периметру. Для попадания в безопасную зону каждый объект сам по себе должен пройти проверку на отсутствие «троянских коней» и прочих опасностей, а затем получить допуск в эту зону. Для этого, в случае программного обеспечения, проводится сертификация на НДВ. Таким образом, сертификат по НДВ – это разрешение на использование конкретного программного продукта (с фиксацией контрольных сумм и образцов программ). Без сертификата на НДВ программы запрещено устанавливать на компьютеры, обрабатывающие информацию ограниченного доступа.

Сертификация СВТ. Более сложным уровнем является такое ПО, которое используется для создания периметра безопасности: средства защиты информации. Эти средства испытываются уже не на закладки, а на способности по защите информации. Для этого существует сертификация по СВТ.

Целью сертификации является гарантирование и официальное подтверждение характеристик программного обеспечения по НДВ или СВТ. Сертификат – это документ, дающий разрешение на использование программного обеспечения (ПО) для решения соответствующих задач Заказчика. Подчеркнем, что наличие сертификата не гарантирует абсолютную защиту информации. Однако, в случае нарушения информационной безопасности, сертификат снимает ответственность (или облегчает ее), подтверждая, что были приняты все юридически определенные меры обеспечения информационной безопасности. Без сертификатов переходить к аттестации и обрабатывать информацию ограниченного доступа не разрешается.

Отметим, что наличие сертификата расширяет и/или сохраняет круг клиентов. Этот сертификат важен для участия в конкурсах, где существуют требования по ИБ. Заказчики часто требуют, как минимум, сертификата по НДВ в системах сертификации ФСТЭК России (государственная) и АйТиСертифика (общественная). Сертификацией имеют право заниматься только специальные испытательные лаборатории, аккредитованные в различных системах сертификации. Сертификаты других организаций не имеют юридической силы. Таким образом, без внешних участников сертификация невозможна. Отметим, что для подготовки к сертификации необходимо разработать специальные документы и документацию на программное обеспечение.

Деятельность корпорации «ЭЛАР» по повышению информационной безопасности «ЭЛАР Саперион»

Реализация «Плана повышения информационной безопасности» в корпорации «ЭЛАР». Прежде всего, была выбрана испытательная лаборатория ЗАО НПО «Эшелон». SAPERION AG предоставили в своем офисе в Берлине все необходимые исходные коды для проведения сертификационных испытаний (специалисты НПО «Эшелон» в феврале 2008 года ездили в Берлин).

В настоящее время в Системе добровольной сертификации средств информационных технологий по требованиям информационной безопасности «АйТиСертифика» Евро-Азиатской ассоциации производителей товаров и услуг в области безопасности получен сертификат № 236, действительный до 28 марта 2011 года. Этот сертификат удостоверяет [4], что «Система управления электронными информационными ресурсами “ЭЛАР Саперион”, функционирующая под управлением ОС Windows 2000 Advanced Server, Windows 2000 Server, Windows XP Professional, Windows 2003 Standard Edition, Windows 2003 Enterprise, SuSE Linux Enterprise Server 8, SuSE Linux Enterprise Server 9, Red Hat Enterprise Linux 4, Solaris 8, Solaris 9, производства компании SAPERION AG, является программным продуктом, предназначенным для ведения электронного архива документов предприятия, и соответствует требованиям руководящего документа “Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей” (Гостехкомиссия России, 1999) по 4 уровню контроля и может использоваться в АС до класса защищенности 1Г включительно». Сертификат выдан на основании результатов испытаний, проведенных испытательной лабораторией ЗАО НПО «Эшелон». Заявитель: ЗАО «ПроСофт-М» (127083, Москва, Петровско-Разумовская аллея, д. 12 а, строение 3, тел. (495) 792-31-31).

Аналогичный сертификат по НДВ-4 получен в ФСТЭК России: сертификат соответствия № 1638, выданный 7 июля 2008 г. Данный сертификат действителен до 7 июля 2011 г. и внесен в российский Государственный реестр сертифицированных средств защиты информации.

Перспективы развития продукта «ЭЛАР Саперион»

В настоящее время намечены следующие перспективы развития:
– доработка продукта с внешними средствами защиты информации;
– сертификация «ЭЛАР Саперион» по СВТ-5;
– проверка взаимодействия «ЭЛАР Саперион» с различным ПО;
– обеспечение совместимости с различными внешними средствами защиты информации (криптография и ЭЦП).
– сертификация «ЭЛАР Саперион» по НДВ и СВТ для более высоких требований безопасности, включая гос. тайну.

Некоторые параметры будут реализовываться под конкретных Заказчиков. Планируется в дальнейшем разработать и/или создать такой комплект ПО, все компоненты которого будут как минимум сертифицированы по НДВ, и аппаратуры, прошедшей спецпроверки и специсследования.

Выводы

Проведенный анализ возможностей компьютерной разведки и защищенности электронных архивов и АС, созданных на основе «ЭЛАР Саперион», показал, что возможно создание АС до класса защищенности 1Г. Для этого, кроме уже полученного сертификата НДВ-4, прежде всего, необходимы: сертификация «ЭЛАР Саперион» по СВТ-5; обеспечение совместимости с различными внешними средствами защиты информации (криптография и ЭЦП). В перспективе, возможна сертификация «ЭЛАР Саперион» по НДВ и СВТ для более высоких требований ИБ по «АС 1Б».

Литература

1. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. – М.: Российский гос. гуманитарный ун-т, 2002. – 399 с.
2. Варламов О.О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ТРТУ. – Тем.выпуск «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2006. – № 7 (62). – С. 216-223.
3. Режим доступа: www.ovar.narod.ru.
4. Материалы сайта корпорации «Электронный архив» (ЭЛАР). – Режим доступа: www.elar.ru.

О.В. Варламов

Комп’ютерна розвідка і створення АС до класу захищеності 1Г на основі сертифікованого ПС «Елар Саперіон»
У статті досліджені можливості і перспективи створення захищених від технічної комп’ютерної розвідки автоматизованих систем на прикладі системи керування інформаційними ресурсами «Елар Саперіон»

Статья поступила в редакцию 17.07.2008.